(in tema di accesso dell'interessato) e che risultano variare da paese a paese; b) le possibilità di uso dei dati a fini diversi da quelli consentiti dal regolamento; c) la qualità –sotto il profilo tecnico– dei dati.

Sulla base di tali indicazioni, in una prima fase il Garante ha inoltrato al Ministero dell'interno una richiesta preliminare di informazioni in relazione agli aspetti sopra evidenziati.

Al fine di completare l'azione richiesta, in una seconda fase il Garante ha deliberato di procedere ai sensi dell'art. 160 del Codice, anche con visita in loco presso i competenti uffici del Ministero dell'interno, centrali e periferici, a una verifica delle informazioni ottenute e riscontrare, in particolare, la sussistenza della base giuridica necessaria per l'inserimento dei dati dattiloscopici nella banca dati centrale e per l'interrogazione del sistema, nonché l'adeguatezza delle misure di sicurezza adottate nel trattamento. Con la medesima deliberazione l'Autorità ha, inoltre, ritenuto necessario svolgere accertamenti più ampi sulla liceità e correttezza dei trattamenti comunque effettuati in attuazione della Convenzione di Dublino.

Gli uffici interessati hanno prestato la propria collaborazione fornendo anche gli elementi e la documentazione richiesti.

Concluse le verifiche, il presente provvedimento viene adottato anche con riguardo alle raccomandazioni formulate dal Garante europeo a seguito del riscontro fornito dall'Autorità al termine della prima fase di accertamenti.

OSSERVA

1. IL SISTEMA EURODAC

Il regolamento n. 2725/2000 istituisce il sistema Eurodac, che si compone dell'unità centrale, di una banca dati centrale informatizzata e dei mezzi di trasmissione dei dati tra gli Stati membri e tale banca dati centrale. Gli Stati membri, direttamente o attraverso l'unità centrale, inseriscono nella banca dati centrale i dati personali (impronte digitali e sesso) appartenenti a tre tipologie di soggetti di età non inferiore a quattordici anni: a) richiedenti asilo; b) stranieri fermati in relazione all'attraversamento irregolare di una frontiera esterna; c) stranieri presenti irregolarmente in uno Stato membro.

I dati vengono inseriti affinché siano confrontati con i dati dei richiedenti l'asilo registrati già presso l'unità centrale, al fine di concorrere alla determinazione dello Stato membro compe-

tente, ai sensi della Convenzione (oggi regolamento) di Dublino, per l'esame di una domanda di asilo presentata in uno Stato membro.

Il regolamento n. 2725/2000 prevede che le norme cui è soggetto il sistema Eurodac si applicano anche alle operazioni effettuate dagli Stati membri, dal momento della trasmissione dei dati all'unità centrale fino all'utilizzazione dei risultati del confronto; specifica inoltre che, fatta salva l'utilizzazione delle informazioni destinate all'Eurodac da parte dello Stato membro d'origine nell'ambito di banche dati istituite ai sensi della propria legislazione nazionale, i dati sulle impronte digitali e le altre informazioni personali possono essere trattati nell'Eurodac solo per gli scopi previsti dall'articolo 15, paragrafo 1, della Convenzione di Dublino (art. 1 reg. n. 2725/2000).

Con riferimento al trattamento dei dati effettuato in Italia, la procedura si articola in due fasi distinte.

La prima si svolge interamente nell'ambito del Dipartimento della pubblica sicurezza del Ministero dell'interno, in particolare attraverso le questure e il Servizio di polizia scientifica, ed è rivolta alla presentazione e ricezione della domanda di asilo, alla raccolta delle informazioni necessarie (tra cui il fotosegnalamento e le verifiche sugli archivi nazionali), alla valutazione dell'ammissibilità della domanda e al suo invio alla Commissione per il riconoscimento dello status di rifugiato, alla trasmissione dei dati alla banca dati centrali Eurodac e, in caso di riscontro positivo, all'Unità Dublino.

Le direttive di carattere tecnico-operativo e di rilievo giuridico vengono impartite dalla Direzione centrale dell'immigrazione e della polizia delle frontiere del Dipartimento della pubblica sicurezza, che cura, su richiesta dell'Unità Dublino, gli approfondimenti necessari ai fini della verifica di eventuali reati a carico dello straniero, nonché ogni altra informazione circa la presenza regolare o meno dello stesso sul territorio nazionale.

La seconda fase fa capo al Dipartimento delle libertà civili e l'immigrazione del Ministero dell'interno, che espleta la procedura di accettazione/rinvio della richiesta prevista dalla Convenzione di Dublino.

In particolare, all'esito degli accertamenti svolti risulta accertata la seguente procedura.

1.1. *Invio dei dati alla banca dati centrale*

Su richiesta dell'ufficio immigrazione presso le questure il Gabinetto provinciale di polizia scientifica della Polizia di Stato effettua il fotosegnalamento dell'interessato al fine dell'inserimento in A.f.i.s. (Automated fingerprint identification system) e in Eurodac, qualora ricorra una delle fattispecie previste dal regolamento n. 2725/2000 sopra precisate alle lett. a), b) e c). Il cartellino fotosegnaletico viene quindi inviato presso il Gabinetto regionale di polizia scientifica, che provvede al controllo della sua qualità tecnica e lo inserisce effettivamente in A.f.i.s. e, se richiesto dal Gabinetto provinciale, nell'Eurodac. L'invio avviene mediante il Servizio di polizia scientifica sito presso il Dipartimento della pubblica sicurezza, designato dall'Italia quale unico punto di accesso nazionale per l'interscambio dei dati con l'unità centrale sita a Bruxelles.

1.2. *Riscontro dell'unità centrale*

In caso di confronto positivo ("risposta pertinente" secondo l'art. 4 reg. n. 2725/2000) l'unità centrale invia i rilievi dattiloscopici al competente gabinetto di polizia scientifica per la conferma della corrispondenza con i rilievi già presenti nella banca dati. A seguito di tale conferma la questura interessata invia la richiesta di asilo, corredata dalla pertinente documentazione, sia alla Commissione per il riconoscimento dello status di rifugiato territorialmente competente a decidere nel merito, sia all'Unità Dublino, ufficio del Dipartimento per le libertà civili e l'immigrazione del Ministero dell'interno che ha il compito di intrattenere i rapporti e curare lo scambio di informazioni con altri omologhi uffici nazionali al fine di individuare lo Stato membro competente a decidere sulla richiesta di asilo. L'Unità Dublino tratta anche i casi in cui la richiesta di asilo è presentata in un altro Stato membro e nel sistema risultano le impronte digitali della persona inserite dall'Italia.

2. PROFILI CRITICI E PRESCRIZIONI DEL GARANTE

Il regolamento n. 2725/2000 e il Codice pongono precisi obblighi in relazione ai trattamenti di dati personali effettuati in funzione dell'applicazione della Convenzione di Dublino.

Le informazioni acquisite, anche attraverso gli accertamenti in loco, hanno permesso di verificare che alcuni di questi obblighi non sono stati attuati correttamente.

In relazione a tali aspetti il Garante rileva pertanto la necessità di impartire ai sensi degli

artt. 154 e 160 del Codice le necessarie modificazioni e integrazioni da apportare al trattamento, di cui, in relazione agli obblighi di controllo ad essa affidati, questa Autorità si riserva di verificare periodicamente l'attuazione ai sensi del medesimo art. 160.

2.1. *Titolare ed eventuali responsabili del trattamento*

Profili critici

La complessità della procedura descritta, con l'intervento di molteplici organi facenti capo a diverse articolazioni del Ministero dell'interno, non consente una chiara individuazione delle diverse responsabilità nel trattamento dei dati per le finalità proprie del sistema Eurodac.

L'imputabilità a più soggetti delle operazioni da svolgere, con la conseguente, mancata individuazione di un unico interlocutore, ha determinato anche ritardi e difficoltà nello stesso svolgimento degli accertamenti deliberati dal Garante.

Prescrizioni

L'art. 13 del regolamento n. 2725/2000 pone precisi obblighi a carico di ciascuno Stato membro, il quale è tenuto a garantire "la legalità del rilevamento delle impronte digitali" e della loro trasmissione all'unità centrale, l'esattezza e l'attualità delle informazioni al momento della trasmissione, "la legalità della registrazione, conservazione, rettifica e cancellazione dei dati nella banca dati centrale", "la legalità dell'uso dei risultati del confronto dei dati sulle impronte trasmessi dall'unità centrale" (paragrafo 1), nonché la sicurezza dei dati in ogni fase del trattamento (paragrafo 2).

Tali obblighi impongono la necessità di identificare chiaramente le responsabilità dei diversi servizi che utilizzano il sistema Eurodac nell'ambito del Ministero dell'interno, ivi compreso il servizio competente per l'accertamento dell'età del soggetto ai fini dell'inserimento delle impronte digitali nel sistema. In particolare, devono essere individuati il titolare (o i co-titolari) del trattamento dei dati, nonché eventuali responsabili; i relativi estremi identificativi devono essere comunicati al Garante, al fine di consentire a questa Autorità di svolgere efficacemente il ruolo di controllo attribuitole (art. 19 reg. cit.).

A questo fine, va posta particolare attenzione al fatto che la descritta attività è "servente" rispetto alla procedura di asilo; pertanto, è richiesto il rigoroso rispetto del principio di finalità del trattamento per tutte le operazioni compiute, dalla raccolta all'utilizzo, alla conservazione e alla comunicazione dei dati.

2.2. *Soggetti che hanno accesso ai dati registrati nell'Eurodac*

Profili critici

L'articolo 15, paragrafo 2, del regolamento Eurodac prevede che ciascuno Stato membro designi "le autorità" che possono accedere ai dati dallo stesso trasmessi e registrati nella banca dati centrale, e comunichi l'elenco di tali autorità alla Commissione europea. Solo tali autorità possono modificare, rettificare, integrare o cancellare i dati da esse inseriti (paragrafo 3).

L'Italia risulta avere designato il Servizio di polizia scientifica che, per sua stessa precisazione, fornisce solo il supporto tecnico alle attività di competenza degli uffici titolari della gestione delle pratiche di asilo e di quelle relative agli accertamenti Eurodac e non è, pertanto, in grado di assumere le responsabilità per le operazioni di trattamento indicate nell'art. 15, nonché per le attività, precisate al punto 2.1, che l'art. 13 del regolamento prevede a carico degli Stati membri e delle autorità da questi designate.

Prescrizioni

Ferme restando le attribuzioni di carattere tecnico del Servizio di polizia scientifica, devono essere individuati dal titolare (o dai co-titolari) del trattamento i soggetti ("le autorità") che assicurino il giusto livello di responsabilità richiesto dagli artt. 13 e 15 del regolamento nelle decisioni di modifica, rettifica, integrazione e cancellazione dei dati inseriti nell'Eurodac.

Sempre al fine dell'espletamento delle necessarie attività di controllo, gli estremi identificativi dei soggetti investiti di tale responsabilità devono essere anch'essi comunicati al Garante, come pure i soggetti che hanno accesso ai risultati delle ricerche in Eurodac, in particolare a quelle relative ai confronti con le categorie b) e c) indicate al punto 1. del presente provvedimento.

2.3. *Finalità dell'accesso al sistema Eurodac*

Profili critici

I rilievi esposti ai punti che precedono evidenziano la mancanza di una chiara definizione dei livelli di responsabilità delle diverse autorità che partecipano al sistema e di una procedura definita e formalizzata che consenta di monitorare il grado di corretta applicazione delle regole che disciplinano il trattamento dei dati da parte dei diversi uffici abilitati, sul territorio nazionale, ad assumere decisioni rilevanti riguardo ai diritti delle persone e a inserire, correggere, richiamare, utilizzare i dati personali conservati nella base di dati gestita dall'unità centrale.

In particolare, per quanto riguarda l'Italia, la Commissione europea e il Garante europeo hanno segnalato l'alto numero di accessi nella base dati centrale giustificati ai sensi dell'art. 18 del regolamento (le cd. "ricerche speciali"), il quale prevede che in ciascuno Stato membro l'interessato può esercitare i diritti di accesso, comunicazione, rettifica e cancellazione dei dati personali che lo riguardano. Nel corso degli accertamenti è risultato che in nessuno dei casi segnalati l'accesso ai dati era stato effettuato su richiesta dell'interessato; né, sono state presentate a questa Autorità istanze di interessati volte a esercitare i diritti conferiti dall'art. 18. In risposta alla richiesta dell'Autorità di verificare la legittimità degli accessi, il Servizio di polizia scientifica presso il Dipartimento della pubblica sicurezza è intervenuto assicurando di avere disattivato per gli uffici periferici tale possibilità di accesso ai dati, che attualmente potrebbe essere effettuato solo presso il Servizio stesso. Nonostante tale assicurazione, e benché il numero di tali casi sia diminuito fortemente, la Commissione europea, nei suoi report trimestrali, ha continuato a segnalare richieste di accesso ai sensi dell'art. 18 non basate su istanze degli interessati.

Prescrizioni

Il titolare e gli eventuali responsabili del trattamento, che vanno individuati ai sensi della prescrizione di cui al punto 2.1, devono adottare un'idonea regolamentazione volta a garantire che l'accesso ai dati gestiti dall'unità centrale sia limitato alle sole finalità previste dal regolamento Eurodac. In particolare, va garantita la conoscibilità di ogni accesso per le *cd.* "ricerche speciali" previste dall'art. 18 del regolamento; deve essere altresì assicurato che solo le autorità competenti per la procedura di asilo possano accedere ai risultati del confronto tra i dati dei soggetti appartenenti alle categorie c) e b) e quelli dei soggetti appartenenti alla categoria a) di cui al punto 1 del presente provvedimento.

2.4. *Formazione del personale e diritti degli interessati*

Profili critici

Con circolare del gennaio 2003 il Dipartimento della pubblica sicurezza ha informato gli uffici di polizia sul territorio dell'imminente entrata in vigore del regolamento Eurodac e ha impartito le relative istruzioni. La circolare fa riferimento alla necessità di garantire i diritti delle persone e reca in allegato un modulo per l'informativa da rendere agli interessati, redatto in più lingue, che viene consegnato alla persona e da questa sottoscritto all'atto del fotosegna-

lamento. Nel corso dell'accertamento del Garante le suddette istruzioni sono state reiterate. Dalle informazioni acquisite non risulta peraltro che finora alcun interessato –direttamente o attraverso il proprio legale o organizzazioni umanitarie– abbia esercitato i diritti conferiti dall'art. 18.

Mancano inoltre informazioni certe sull'effettivo utilizzo del modulo da parte di tutte le questure.

Prescrizioni

Il titolare e gli eventuali responsabili del trattamento devono garantire un'adeguata formazione del personale, in particolare in merito all'uso legittimo delle cd. "ricerche speciali", e assicurare che l'intera procedura, dall'identificazione della persona alla decisione sulla richiesta di asilo avvenga nel rispetto della dignità dell'interessato.

In coerenza con quanto previsto dal regolamento Eurodac, il titolare e gli eventuali responsabili del trattamento devono assicurare il puntuale rispetto di quanto previsto nell'articolo 18, fornendo le informazioni previste e precisando le relative procedure al fine di mettere l'interessato nella condizione di esercitare i diritti riconosciutigli. Al riguardo, l'informativa non risulta del tutto adeguata rispetto a quanto prescritto dall'art. 18, con particolare riferimento all'indicazione del titolare (o co-titolari) del trattamento dai dati (l'informativa attualmente fornita indica come responsabile del trattamento dei dati il Gabinetto di polizia scientifica che procede all'operazione di fotosegnalamento), degli specifici diritti che possono essere esercitati dagli interessati e delle autorità (Garante e autorità giudiziaria) a cui presentare un eventuale ricorso.

Si rende quindi necessario aggiornare il testo dell'informativa attualmente fornita con l'inserimento di tali ulteriori informazioni.

2.5. *Misure di sicurezza*

In relazione agli elementi acquisiti, la particolare natura dei dati induce a evidenziare la necessità che, ferme restando le cautele attualmente previste dagli artt. 31 e ss. e dall'Allegato B. al Codice, vengano adottate, da parte degli organi interessati dalla procedura, ulteriori misure e accorgimenti, di seguito indicati, volti a rafforzare il livello di protezione delle informazioni oggetto di trattamento, anche in attuazione dell'obbligo di garantire la sicurezza dei dati prima, durante e dopo la trasmissione all'unità centrale, nonché dei dati ricevuti dall'unità centrale che l'art. 13, paragrafo 2, del regolamento n. 2725/2000 pone a carico di ogni Stato membro.

2.5.1. *Credenziali di autenticazione presso il Servizio di polizia scientifica*

Profili critici

Presso il Servizio di polizia scientifica del Dipartimento della pubblica sicurezza vengono conservati i log file relativi al tracciamento delle operazioni effettuate sulle impronte digitali destinate a confluire in Eurodac (e in A.f.i.s) dai gabinetti provinciali e regionali della polizia scientifica. Nei log vengono memorizzate le attività svolte, il nome dell'utente, il codice della postazione client di provenienza della richiesta, il numero originario identificativo dell'operazione effettuata dal client e il codice A.f.i.s..

L'accesso alla sala macchine che ospita il server centrale è consentito mediante badge profilato.

L'accesso degli amministratori al database dei log Eurodac (e A.f.i.s.) avviene mediante credenziali di autenticazione (username e password) condivise tra il personale dell'area Gruppo sistemistico sezione A.f.i.s..

Prescrizioni

Per l'accesso al database Eurodac (e A.f.i.s.), a ogni incaricato deve essere assegnata o associata individualmente almeno una credenziale di autenticazione costituita da un codice utente e da una parola chiave composta da non meno di otto caratteri, che deve essere modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni tre mesi.

2.5.2. *Conservazione dei fascicoli cartacei presso l'Unità Dublino*

Profili critici

Presso l'Unità Dublino del Dipartimento per le libertà civili e l'immigrazione vengono conservati, in numero di oltre 90.000, i fascicoli cartacei relativi ai soggetti i cui dati personali vengono trattati dall'Unità in relazione ai compiti da questa svolti nell'ambito della procedura che disciplina Eurodac. Si tratta di dati anche biometrici (le impronte digitali contenute nei cartellini dattiloscopici) e di carattere giudiziario, tra i quali le informazioni relative agli interessati acquisite dal Centro elaborazioni dati del Dipartimento della pubblica sicurezza.

Allo stato, i fascicoli sono sistemati in armadi privi di chiusura collocati in stanze non chiuse a chiave. Sono in corso attività volte a dotare di serrature gli armadi e le stanze.

É installato un impianto di rilevazione incendi e un sistema di videosorveglianza, che entra in funzione al di fuori dell'orario di lavoro del personale.

Prescrizioni

I dati personali contenuti nei fascicoli cartacei devono essere custoditi e controllati con modalità che riducano al minimo i rischi di distruzione o perdita o di accesso non autorizzato.

L'accesso ai locali ove sono custoditi i fascicoli va consentito previa adozione di un sistema di controllo basato sull'utilizzo di una tessera individuale (ad esempio, un badge profilato) a disposizione dei soli soggetti incaricati del trattamento delle informazioni.

I fascicoli devono essere collocati in armadi ignifughi dotati di idonee serrature di sicurezza.

I varchi di accesso ai locali devono essere anch'essi dotati di idonee serrature di sicurezza.

2.5.3 *Trattamento dei dati con strumenti elettronici presso l'Unità Dublino*

Profili critici

Lo scambio di informazioni e documentazione con uffici esterni all'Unità (omologhi uffici di Stati membri e questure) avviene mediante posta elettronica certificata e non, posta tradizionale e fax, con esclusione, quanto al fax, della trasmissione dei cartellini dattiloscopici, causa la cattiva risoluzione dell'immagine.

L'accesso alle postazioni informatiche da parte del personale avviene mediante credenziali di autenticazione personale di dominio Windows.

L'accesso all'applicazione web DubliNET, attraverso cui l'Unità gestisce i dati e le comunicazioni con gli Stati membri, avviene attraverso un sito non Ssl (Secure Socket Layer) e, quindi, senza certificato di sicurezza.

Le credenziali di autenticazione (username e password) per l'accesso all'applicazione DubliNET sono condivise fra i vari operatori.

La documentazione scaricabile dal sistema DubliNET (ad esempio, in formato Pdf), ivi compresi i cartellini dattiloscopici, viene firmata digitalmente dal mittente, ma le postazioni informatiche in uso al personale dell'Unità non sono dotate del sistema di verifica della firma digitale (all'interno del file nell'area dedicata alla firma digitale risulta presente un punto interrogativo).

Gli accessi all'applicazione DubliNET e le operazioni compiute sui dati vengono tracciate.

Prescrizioni

Lo scambio di informazioni e documentazione da e verso l'Unità Dublino deve avvenire con modalità che assicurino la provenienza della comunicazione e l'integrità del suo contenuto.

Le comunicazioni devono quindi avvenire esclusivamente attraverso posta elettronica certificata e i documenti trasmessi devono essere cifrati.

Per l'accesso all'applicazione web DubliNET, a ogni incaricato deve essere assegnata o associata individualmente almeno una credenziale di autenticazione costituita da un codice utente e da una parola chiave composta da non meno di otto caratteri, che deve essere modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni tre mesi.

3. TERMINE PER ATTUARE LE PRESCRIZIONI DEL GARANTE

Attesa la particolare delicatezza dei dati in questione, il Garante constata la necessità che le prescritte modificazioni e integrazioni da apportare al trattamento siano adottate entro termini brevi, decorrenti dalla data di ricezione del presente provvedimento, che risulta congruo fissare:

a) in trenta giorni, relativamente alle misure di sicurezza concernenti l'adozione delle credenziali individuali di autenticazione da parte del personale dell'area Gruppo sistemistico sezione A.f.i.s. del Servizio di Polizia scientifica del Dipartimento della pubblica sicurezza e degli operatori dell'Unità Dublino del Dipartimento per le libertà civili e l'immigrazione;

b) in sei mesi, relativamente alle altre modificazioni e integrazioni, ivi comprese le ulteriori misure di sicurezza prescritte (punto 2.5).

Il Ministero, che allo stato risulta titolare del trattamento, è invitato a fornire riscontro al decorso di ciascuno di tali termini circa l'attuazione delle presenti prescrizioni.

TUTTO CIÒ PREMESSO IL GARANTE

1) ai sensi degli artt. 154, comma 1, lett. c) e 160 del Codice dispone che il Ministero dell'interno adotti le prescritte modificazioni e integrazioni al trattamento dei dati personali effettuati in attuazione del regolamento n. 2725/2000 istitutivo del sistema Eurodac e della Convenzione di Dublino relativamente a:

   a) individuazione e comunicazione al Garante degli estremi identificativi del titolare (o co-titolari) e eventuali responsabili del trattamento, con indicazione dei compiti e delle responsabilità dei vari soggetti che effettuano il trattamento dei dati nell'ambito della procedura, al fine di assicurare la liceità del trattamento, la correttezza e sicurezza dei dati e il rigoroso rispetto del principio di finalità del trattamento per tutte

le operazioni compiute, dalla raccolta all'utilizzo, alla conservazione e alla comunicazione dei dati (punto 2.1);

b) individuazione e comunicazione al Garante degli estremi identificativi dei soggetti "le autorità") che assicurino il livello di responsabilità richiesto dagli artt. 13 e 15 del regolamento n. 2725/2000 nelle decisioni di modifica, rettifica, integrazione e cancellazione dei dati registrati presso la banca dati centrale e che possono accedere ai risultati delle ricerche nel sistema, in particolare a quelle relative ai confronti con le categorie b) e c) indicate al punto 1 del presente provvedimento (punto 2.2);

c) adozione di una idonea regolamentazione volta a garantire che l'accesso ai dati gestiti dall'unità centrale sia limitato alle sole finalità previste dal regolamento n. 2725/2000 e alle sole autorità competenti per la procedura di asilo, con particolare riferimento alle cd. "ricerche speciali" di cui all'art. 18 del regolamento (punto 2.3);

d) formazione del personale in relazione al trattamento dei dati effettuato nel corso della procedura, con particolare riferimento all'uso legittimo delle cd. "ricerche speciali"; aggiornamento del testo dell'informativa da rendere all'interessato con particolare riferimento all'inserimento dell'indicazione del titolare (o co-titolari) del trattamento dei dati e degli specifici diritti che possono essere esercitati dagli interessati e delle autorità (Garante e autorità giudiziaria) a cui presentare un eventuale ricorso (punto 2.4);

2) ai sensi degli artt. 154, comma 1, lett. c) e 160 del Codice dispone che il Ministero dell'interno adotti adeguate misure di sicurezza nel trattamento dei dati, volte a rafforzare il livello di protezione delle informazioni trattate nell'ambito del sistema Eurodac, con particolare riferimento a (punto 2.5):

a) assegnazione al personale dell'area Gruppo sistemistico sezione A.f.i.s. del Servizio di Polizia scientifica del Dipartimento della pubblica sicurezza e del personale dell'Unità Dublino del Dipartimento per le libertà civili e l'immigrazione di credenziali individuali di autenticazione costituite da un codice utente e da una parola chiave composta da non meno di otto caratteri, che deve essere modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni tre mesi;

b) conservazione dei fascicoli cartacei presso l'Unità Dublino del Dipartimento per le

libertà civili e l'immigrazione in armadi ignifughi dotati di serrature di sicurezza collocati in locali con accesso consentito previa adozione di un sistema di controllo basato sull'utilizzo di una tessera individuale (ad esempio, un badge profilato) a disposizione dei soli soggetti incaricati del trattamento delle informazioni e con varchi dotati di idonee serrature di sicurezza;

c) trattamento dei dati con strumenti elettronici presso la medesima Unità mediante comunicazioni basate sull'uso esclusivo di posta elettronica certificata e sulla trasmissione di documenti cifrati;

3) ai sensi delle medesime disposizioni prescrive che le suesposte modificazioni e integrazioni da apportare al trattamento siano adottate entro il termine, decorrente dalla data di ricezione del presente provvedimento, di trenta giorni relativamente alle misure di sicurezza concernenti l'adozione delle credenziali individuali di autenticazione da parte del personale dell'area Gruppo sistemistico sezione A.f.i.s. del Servizio di Polizia scientifica del Dipartimento della pubblica sicurezza e del personale dell'Unità Dublino del Dipartimento per le libertà civili e l'immigrazione, e di sei mesi relativamente alle altre modificazioni e integrazioni, ivi comprese le ulteriori misure di sicurezza prescritte, fornendo riscontro a questa Autorità circa la loro attuazione al decorso dei medesimi termini.

Roma, 29 maggio 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

27. RECEPIMENTO NORMATIVO IN TEMA DI DATI DI TRAFFICO TELEFONICO E TELEMATICO (*)

ALLEGATO A

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196, di seguito, "Codice");

Visti in particolare gli artt. 17, 123 e 132, comma 5, del Codice;

Vista la deliberazione del 19 settembre 2007 con la quale l'Autorità ha avviato una procedura di consultazione pubblica su un documento, adottato in pari data, riguardante "Misure e accorgimenti a garanzia degli interessati in tema di conservazione di dati di traffico telefonico e telematico per finalità di accertamento e repressione di reati" e pubblicato, unitamente alla medesima deliberazione, sul sito web dell'Autorità;

Visti i commenti e le osservazioni pervenuti a questa Autorità a seguito della consultazione pubblica per la quale era stato fissato il termine del 31 ottobre 2007;

Considerate le risultanze dei diversi incontri, anche di carattere tecnico, intercorsi con alcune associazioni di categoria che lo avevano richiesto;

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Francesco Pizzetti;

PREMESSO

1. CONSIDERAZIONI PRELIMINARI

Il trattamento dei dati di traffico telefonico e telematico presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

(*) Gazzetta Ufficiale 13 agosto 2008, n. 189 [doc. *web* n. 1538237], in inglese [doc. *web* n. 1542849]

Tali informazioni hanno una natura particolarmente delicata e la loro impropria utilizzazione può avere importanti ripercussioni sulla sfera personale di più soggetti interessati; possono avere un'"accentuata valenza divulgativa di notizie caratterizzanti la personalità dell'autore" e la loro conoscibilità richiede adeguate garanzie (cfr., fra l'altro, Corte cost. 11 marzo 1993, n. 81 e 14 novembre 2006 n. 372).

I dati relativi al traffico telefonico e telematico dovrebbero peraltro riguardare solo alcune caratteristiche esteriori di conversazioni, chiamate e comunicazioni, senza permettere di desumerne i contenuti.

Inoltre, le stesse caratteristiche esteriori permettono di individuare analiticamente quando, tra chi e come sono intercorsi contatti telefonici o per via telematica, o sono avvenute determinate attività di accesso all'informazione in rete e persino il luogo dove si trovano i detentori di determinati strumenti.

L'intensità dei flussi di comunicazione comporta la formazione e, a volte, la conservazione di innumerevoli informazioni che consentono di ricostruire nel tempo intere sfere di relazioni personali, professionali, commerciali e istituzionali, e di formare anche delicati profili interpersonali. Ciò, specie quando i dati sono conservati massivamente dai fornitori per un periodo più lungo di quello necessario per prestare servizi a utenti e abbonati, al fine di adempiere a un distinto obbligo di legge collegato a eccezionali necessità di giustizia.

Per le comunicazioni telematiche, poi, si pongono ulteriori e più specifiche criticità rispetto alle comunicazioni telefoniche tradizionalmente intese, in quanto il dato apparentemente "esterno" a una comunicazione (ad es., una pagina web visitata o un indirizzo Ip di destinazione) spesso identifica o rivela nella sostanza anche il suo contenuto: può permettere, quindi, non solo di ricostruire relazioni personali e sociali, ma anche di desumere particolari orientamenti, convincimenti e abitudini degli interessati.

Eventuali abusi (quali quelli emersi nel recente passato, allorché sono stati constatati gravi e diffusi fatti di utilizzazione illecita di dati), possono comportare importanti ripercussioni sulla sfera privata degli individui o anche violare specifici segreti attinenti a determinate attività, relazioni e professioni.

Emerge quindi la necessità, in attuazione di quanto previsto per legge, di assicurare che la con-

servazione di tali dati da parte dei fornitori, laddove essa sia necessaria per prestare un servizio o in quanto imposta dalla legge, avvenga comunque in termini adeguati per garantire una tutela maggiormente efficace dei diritti e delle libertà delle persone.

Per tali motivi, a prescindere dalle garanzie previste in termini più generali nell'ordinamento anche sul piano costituzionale e processuale, il legislatore all'art. 132 del Codice ha demandato al Garante per la protezione dei dati personali l'individuazione delle misure e degli accorgimenti che i fornitori dei servizi di comunicazione elettronica devono adottare a fronte della conservazione dei dati di traffico telefonico e telematico, allo stato prescritta per finalità di accertamento e repressione dei reati.

Il presente provvedimento è rivolto appunto a individuare le elevate cautele che devono essere osservate dai fornitori nella formazione e nella custodia dei dati del traffico telefonico e telematico.

Prima di indicare quali cautele risultano necessarie a seguito del complesso procedimento di accertamento curato dal Garante, sono opportune alcune altre premesse sull'attuale quadro normativo, sui fornitori e sui dati personali coinvolti.

2. QUADRO DI RIFERIMENTO

2.1. *Normativa comunitaria*

La direttiva europea n. 2002/58/Ce, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, impone agli Stati membri di proteggere la riservatezza delle comunicazioni elettroniche e vieta la conservazione dei dati relativi al traffico generati nel corso delle comunicazioni, a eccezione della conservazione espressamente autorizzata per i fini indicati nella direttiva medesima.

La direttiva riguarda (art. 3) il trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione. I dati relativi al traffico sono definiti, in questa sede, quali quelli sottoposti a trattamento "ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione" (cfr. art. 2 e considerando n. 15 della direttiva 2002/58/Ce).

La medesima direttiva, nell'imporre agli Stati membri l'adozione di disposizioni di legge nazionali che assicurino la riservatezza delle comunicazioni effettuate tramite la rete pubblica di

comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, pone l'accento sui dati di traffico generati dai servizi medesimi (art. 5); tali dati, trattati e memorizzati dal fornitore della rete pubblica o del servizio pubblico di comunicazione elettronica, devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione, fatte salve alcune tassative eccezioni (cfr. art. 6, par. 2 , 3 e 5 e art. 15, par. 1; v., fra gli altri, il Parere n. 1/2003 sulla memorizzazione ai fini di fatturazione dei dati relativi al traffico, adottato il 29 gennaio 2003 dal Gruppo dei garanti europei per la tutela dei dati personali).

L'art. 15, par. 1, della direttiva consente che gli Stati membri possano adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui ai predetti articoli 5 e 6 solo quando tale restrizione costituisca "una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioé della sicurezza dello Stato), della difesa, della sicurezza pubblica e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica". A tal fine, gli Stati membri possono, tra l'altro, adottare misure legislative le quali prevedano che, per tali motivi, i dati siano conservati per un periodo di tempo limitato.

2.2. *Normativa nazionale*

La direttiva 2002/58/Ce è stata recepita con il Codice in materia di protezione dei dati personali (Titolo X ("Comunicazioni elettroniche"); cfr. art. 184). Nel Capo I di tale Titolo, intitolato "Servizi di comunicazione elettronica", è stata introdotta una nuova disciplina sulla conservazione dei dati di traffico telefonico.

Da un lato, l'art. 123 del Codice ha ridotto a sei mesi il previgente limite temporale per la conservazione dei dati di traffico telefonico per finalità di fatturazione, pagamenti in caso di interconnessione e di commercializzazione di servizi, termine che era in precedenza individuabile nella misura massima di cinque anni in base a quanto previsto dal d.lg. n. 171/1998.

Dall'altro, l'art. 132 del medesimo Codice, modificato prima della sua entrata in vigore (d.l. 24 dicembre 2003, n. 354, convertito in l., con modificazioni, dall'art. 1 l. 26 febbraio 2004, n. 45) ha introdotto un distinto obbligo per i fornitori di servizi di comunicazione elettronica di conservare per finalità di accertamento e repressione dei reati dati di traffico telefonico relativi ai servizi offerti.